

**This Page Is Inserted by IFW Operations  
and is not a part of the Official Record**

## **BEST AVAILABLE IMAGES**

**Defective images within this document are accurate representations of the original documents submitted by the applicant.**

**Defects in the images may include (but are not limited to):**

- **BLACK BORDERS**
- **TEXT CUT OFF AT TOP, BOTTOM OR SIDES**
- **FADED TEXT**
- **ILLEGIBLE TEXT**
- **SKEWED/SLANTED IMAGES**
- **COLORED PHOTOS**
- **BLACK OR VERY BLACK AND WHITE DARK PHOTOS**
- **GRAY SCALE DOCUMENTS**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**



## DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets <sup>7</sup> : <b>H04Q 7/38</b>	<b>A1</b>	(11) Numéro de publication internationale: <b>WO 00/25546</b>
		(43) Date de publication internationale: 4 mai 2000 (04.05.00)

(21) Numéro de la demande internationale: PCT/FR99/02233

(22) Date de dépôt international: 21 septembre 1999 (21.09.99)

(30) Données relatives à la priorité:

98/13440 27 octobre 1998 (27.10.98) FR

(71) Déposant (pour tous les Etats désignés sauf US): GEM-PLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (US seulement): LE GALL, Jean, Pierre [FR/FR]; Chemin Saint Marc, F-13790 Rousset (FR). CHEW, Gary [SG/FR]; 397 Rue Paradis, F-13008 Marseille (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos Cedex (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Avec rapport de recherche internationale.

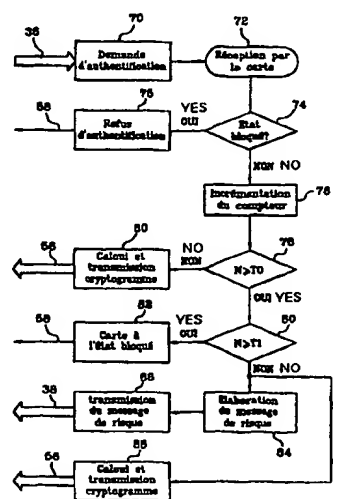
(54) Title: MOBILE METHOD AND SYSTEM FOR MANAGING RISK IN A MOBILE TELEPHONE NETWORK.(54) Titre: PROCEDE ET SYSTEME DE GESTION DU RISQUE DANS UN RESEAU DE TELEPHONIE MOBILE

## (57) Abstract

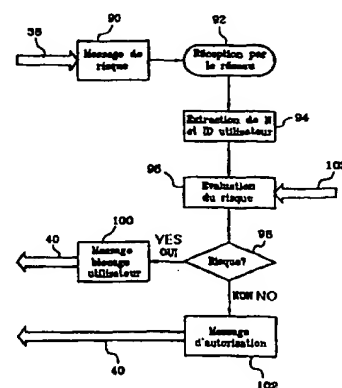
The invention concerns mobile telephone system networks, characterised in that the electronic chip card (22, SIM) comprises means (32) for authorising or not the computation of a cryptographic certificate and transmitting (56) it to the network when certain conditions are fulfilled or not and for transmitting to the network a message (38) requesting to assess risk when other conditions are fulfilled. Moreover, the network (54) comprises means (34) for assessing said risk on the basis of data contained in the message (38) requesting assessment of the risk and user-specific parameters and for sending a message (40) to said means (32) authorising or not the computation and transmission of the cryptographic certificate.

## (57) Abrégé

L'invention concerne les réseaux de téléphonie mobile. L'invention réside dans le fait que la carte à puce électronique (22, SIM) comprend des moyens (32) pour autoriser ou non le calcul d'un certificat cryptographique et sa transmission (56) au réseau lorsque certaines conditions sont remplies ou non et pour transmettre au réseau un message (38) de demande d'évaluation du risque lorsque d'autres conditions sont remplies. Par ailleurs, le réseau (54) comprend des moyens (34) pour évaluer ledit risque en fonction des informations contenues dans le message (38) de demande d'évaluation du risque et de paramètres spécifiques à l'utilisateur et pour envoyer un message (40) auxdits moyens (32) pour autoriser ou non le calcul et la transmission du certificat cryptographique.



70...REQUESTING AUTHENTICATION  
72...RECEPTION BY CARD  
74...OFF STATE ?  
75...AUTHENTICATION DENIED  
76...INCREMENTING COUNTER  
78...COMPUTING AND TRANSMITTING CRYPTOGRAM  
80...CARD IN OFF STATE  
82...PREPARING RISK MESSAGE  
84...TRANSMITTING RISK MESSAGE  
86...COMPUTING AND TRANSMITTING CRYPTOGRAM



90...RISK MESSAGE  
92...RECEPTION BY NETWORK  
94...EXTRACTING N AND USER ID  
96...ASSESSING RISK  
98...RISK ?  
100...MESSAGE FOR BLOCKING USER  
102...AUTHORISATION MESSAGE

# **UNIQUEMENT A TITRE D'INFORMATION**

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

**PROCEDE ET SYSTEME DE GESTION DU RISQUE  
DANS UN RESEAU DE TELEPHONIE MOBILE**

L'invention concerne les réseaux de téléphonie mobile et, plus particulièrement dans de tels réseaux, un procédé et un système pour gérer le risque encouru par l'opérateur du réseau de téléphonie mobile en présence d'usagers susceptibles d'outrepasser leurs droits ou d'opérations anormales.

Un système de téléphonie mobile du type GSM (acronyme de l'expression anglo-saxonne Group Special Mobile), comprend un réseau de téléphonie mobile, géré par un opérateur, qui permet de connecter entre eux des usagers munis chacun d'un combiné mobile ME (acronyme de l'expression anglo-saxonne "Mobile Equipment"), chaque combiné comprenant notamment une carte à puce électronique SIM (acronyme de l'expression anglo-saxonne "Subscriber Identification Module").

Dans un tel système de téléphonie mobile, il est prévu un certain nombre d'opérations pour authentifier la carte SIM par le réseau, au moment de la mise en marche du combiné, ainsi qu'à tout autre moment de la communication téléphonique.

A cet effet, le procédé d'authentification comprend les étapes suivantes consistant à :

(1) remettre à zéro la carte par le combiné ou appareil mobile ME et transmettre l'identité de la carte SIM au réseau,

(2) obtenir du réseau un nombre aléatoire NA à la demande du combiné ME,

(3) transmettre le nombre aléatoire NA à la carte SIM par le combiné ME,

(4) calculer dans la carte SIM un premier certificat cryptographique CC1 ou cryptogramme selon un algorithme prédéfini AL, à partir du nombre

aléatoire NA fourni par le réseau et d'une clé secrète CS interne à la carte SIM,

5 (5) transmettre au réseau, via le combiné ME, le premier certificat cryptographique CC1 calculé par la carte SIM,

(6) calculer un deuxième certificat cryptographique CC2 par le réseau selon le même algorithme AL que celui de la carte SIM, à partir du nombre aléatoire NA envoyé à la carte SIM et de la clé interne secrète CS qui est  
10 connue du réseau par l'identité de la carte SIM,

(7) comparer le deuxième certificat cryptographique CC2 au premier certificat cryptographique CC1 et,

(8) autoriser la transaction si la comparaison est positive ou l'interdire dans le cas contraire.

15 Un tel procédé d'authentification permet de vérifier que le porteur du combiné ME auquel la carte SIM est associée est bien autorisé à entrer en communication par l'intermédiaire du réseau. Cependant, ce procédé ne permet pas de prendre en compte d'autres  
20 conditions qui seraient à remplir pour autoriser une entrée en communication. L'une des conditions supplémentaires à remplir pourrait être, dans le cas d'une carte à prépaiement, que le montant restant au crédit du porteur du combiné soit supérieur à un  
25 certain seuil prédéterminé, cette condition tendant à limiter le risque d'un défaut de paiement éventuel.

Par ailleurs, les procédés d'authentification mis en oeuvre actuellement ne permettent pas de détecter des demandes d'accès répétées d'un fraudeur à l'aide  
30 d'un combiné volé et, a fortiori, de bloquer cet accès après un certain nombre de demandes d'accès.

Un but de la présente invention est donc, de mettre en oeuvre un procédé d'authentification d'une carte d'abonné à un réseau de télécommunications qui permet  
35 de prendre en compte différentes conditions,

éventuellement évolutives, de manière à gérer ou limiter les risques encourus par l'opérateur en autorisant l'accès au réseau.

5 Ce but est atteint en introduisant des moyens dans la carte SIM du combiné et dans le serveur du réseau ; ces moyens communiquent entre eux par des messages transmis sur une voie de télécommunication de service telle que celle utilisée actuellement pour le service des Messages Courts, plus connu sous l'acronyme anglo-saxon SMS pour "Short Message Service".

10 L'invention concerne donc un système de gestion du risque dans un réseau de téléphonie mobile équipé d'un dispositif de service de messages, les combinés mobiles comportant chacun une carte à puce électronique SIM capable de calculer un certificat cryptographique d'authentification à partir d'une valeur fournie par le réseau, caractérisé :

20 - en ce que la carte à puce électronique comprend des moyens pour autoriser ou non le calcul d'un certificat cryptographique et sa transmission au réseau lorsque certaines conditions sont remplies ou non et pour transmettre au réseau un message de demande d'évaluation du risque lorsque d'autres conditions sont remplies, et

25 - en ce que le réseau comprend des moyens pour évaluer ledit risque en fonction des informations contenues dans le message de demande d'évaluation du risque et de paramètres spécifiques à l'utilisateur du combiné mobile et pour envoyer un message auxdits moyens de la carte à puce électronique pour autoriser ou non le calcul et la transmission du certificat cryptographique.

30 L'invention concerne également un procédé pour mettre en oeuvre le système de gestion du risque défini ci-dessus, caractérisé en ce qu'il comprend, dans la

carte à puce électronique, les étapes suivantes consistant à :

5 (a) vérifier l'état bloqué ou non de la carte à puce électronique pour refuser ou non la demande d'authentification ;

(b) dans le cas d'autorisation de la demande d'authentification, compter le nombre  $N$  de demandes d'authentification de la carte à puce électronique par le réseau,

10 (c) comparer le nombre  $N$  de demandes d'authentification à un premier seuil  $T_0$ ,

(d) calculer un certificat cryptographique si  $N < T_0$  et le transmettre au réseau,

15 (e) comparer le nombre  $N$  à un deuxième seuil  $T_1$  si  $N \geq T_0$ ,

(f) mettre la carte à puce électronique à l'état bloqué si  $N \geq T_1$ , et

20 (g) calculer un certificat cryptographique et élaborer un message de demande d'évaluation du risque et les transmettre au réseau si  $T_0 < N \leq T_1$ .

Le procédé ci-dessus est caractérisé en ce que, dans le réseau, il comprend les étapes supplémentaires suivantes consistant à :

25 (h) analyser le message de demande d'évaluation du risque transmis par la carte à puce électronique,

(i) évaluer le risque en fonction des résultats de l'analyse selon l'étape précédente (h) et de paramètres spécifiques à l'utilisateur du combiné mobile, et

30 (j) élaborer un message de réponse et le transmettre à la carte à puce électronique.

D'autres caractéristiques et avantages de la présente invention apparaîtront à lecture de la description suivante d'un exemple particulier de réalisation, ladite description étant faite en relation  
35 avec les dessins joints dans lesquels :

- la figure 1 est un diagramme montrant schématiquement les flux d'informations entre les différents éléments du réseau de téléphonie mobile,

- la figure 2 est un diagramme fonctionnel d'un module de gestion du risque associé à la carte à puce électronique d'un combiné mobile, et

- la figure 3 est un diagramme fonctionnel d'un module de gestion du risque associé au réseau de téléphonie mobile.

10 Un réseau de téléphonie mobile comprend schématiquement trois parties A, B et C qui sont délimitées verticalement par deux traits pointillés 10 et 12.

15 La partie centrale B correspond à la transmission bilatérale radioélectrique des communications, entre un combiné mobile 14 (ou ME) et une station de base 16 (ou BS correspondant à l'acronyme de l'expression anglo-saxonne "Base Station") associée à un équipement de messagerie 18 (ou SMSC correspondant à l'acronyme de l'expression anglo-saxonne "Short Message Service Center") qui fournit le service SMS (acronyme de l'expression anglo-saxonne "Short Message Service") défini ci-dessus dans le préambule.

25 La partie C correspond au réseau de téléphonie mobile 54 et comprend notamment un système de commutation 20 (ou MSC pour l'expression anglo-saxonne "Mobile Switching Center"), un module d'enregistrement des abonnés 50 (ou HLR pour l'expression anglo-saxonne "Home Location Register") et un module d'authentification 52 (ou AC pour l'expression anglo-saxonne "Authentication Center"). Le module d'enregistrement d'abonnés 50 contient les caractéristiques identifiant chacun des abonnés. Le module d'authentification 52 contient la clé secrète CS  
35 de chaque abonné, émet des nombres aléatoires NA,

calcule les certificats cryptographiques CC2 et compare le certificat cryptographique CC2 au certificat cryptographique CC1 calculé par la carte SIM.

La partie A correspond aux caractéristiques de l'abonné au réseau et comprend une carte SIM 22 qui est mise en place dans le combiné mobile 14. Les informations sont échangées bilatéralement entre la carte SIM 22 et le combiné mobile 14 (flèche 24), entre le combiné mobile 14 et la station de base 16 (flèche 26), entre la station de base 16 et l'équipement de messagerie 18 (flèche 28) et entre l'équipement de messagerie 18 et le réseau 54 (flèche 30).

Pour authentifier la carte SIM et autoriser une communication, les étapes (1) à (8) du procédé décrit dans le préambule, sont exécutées à l'initiative de l'équipement mobile.

Selon l'invention, la carte SIM 22 et le réseau 54 sont complétées pour mettre en oeuvre le procédé de gestion du risque. A cet effet, la carte SIM 22 et le réseau 54 sont complétés chacun par un module dit de gestion du risque, référencé 32 pour la carte et 34 pour le serveur.

Le module carte 32 contient les éléments relatifs à l'abonné, tandis que le module réseau 34 contient les éléments qui sont nécessaires au réseau 54 pour interpréter les informations fournies par le module carte et prendre une décision quant à l'authentification à exécuter en fonction de certains critères.

Plus précisément, la demande d'authentification 36 de la carte par le réseau 54 par l'envoi d'un nombre aléatoire NA à la carte 22 par l'intermédiaire du combiné mobile 14, déclenche les opérations du module 32 de la carte 22. Ce module analyse cette demande en

fonction de critères relatifs à l'abonné et prend une décision selon les étapes du diagramme de la figure 2.

Dans le cas où le module 32 détecte un risque, un message d'évaluation du risque 38 est transmis au réseau 54 et plus particulièrement au module de gestion 34 qui prend une décision selon les étapes du diagramme de la figure 3. Cette décision ou réponse est transmise à la carte 22 par un message 40 qui a pour résultat, soit d'autoriser l'authentification de la carte selon la procédure habituelle, soit de bloquer cette authentification et plus généralement de bloquer la carte.

Sur le diagramme de la figure 2, une demande d'authentification (étape 70) de la carte par le terminal commence par la transmission à la carte d'un aléa ou nombre aléatoire NA selon la flèche 36 via le combiné ME. Cette demande d'authentification est reçue par la carte (étape 72) pour être traitée par le module de gestion du risque 32.

Ce module de gestion 32 comprend principalement :

- un registre d'état RMS pour indiquer l'état de la carte, bloqué ou non, (RMS étant l'acronyme de l'expression anglo-saxonne "Risk Management Status"),
- un compteur CAC pour compter le nombre N de demandes d'authentification (CAC étant l'acronyme de l'expression anglo-saxonne "Cumulative Authentication Counter"),

- des comparateurs pour comparer la valeur N du compteur CAC à des seuils T0 et T1 tels que  $T0 < T1$ .

Dans le cas où le registre RMS est à l'état bloqué (étape 74), l'authentification est refusée (étape 75) de sorte que le module de gestion 32 bloque la carte par un signal 58.

Dans le cas où le registre RMS n'est pas à l'état bloqué, cette demande d'authentification incrémente le

compteur CAC (étape 76) d'une unité. La valeur N résultant de cette incrémentation est comparée (étape 78) au premier seuil T0.

5 Si cette valeur incrémentée est inférieure à T0, le module 32 calcule (étape 80) le premier certificat cryptographique CC1 (aussi appelé cryptogramme) selon l'algorithme AL à partir de la valeur aléatoire NA. Ce certificat CC1 est transmis (56) au réseau 54.

10 Si cette valeur incrémentée est égale ou supérieure à T0, elle est comparée au deuxième seuil T1 (étape 80). Si elle est égale ou supérieure à T1, le registre RMS est mis à l'état bloqué (étape 82) et l'authentification est refusée selon l'étape 76 de sorte que le module de gestion 32 bloque la carte par  
15 le signal 58.

Si la valeur incrémentée est inférieure à T1, le module de gestion élabore (étape 84) un message de demande d'évaluation du risque et le transmet (étape 86) au réseau 54 selon la flèche 38 pour y être traité  
20 selon le diagramme de la figure 3.

Par ailleurs, comme le deuxième seuil T1 n'est pas atteint, le blocage de la carte n'est pas envisagé, de sorte que la carte calcule le certificat cryptographique CC1 (étape 88) et le transmet (56) au  
25 réseau 54.

Le message de demande d'évaluation du risque 38 est transmis au réseau 54 selon le format SMS pour y être reçu (étapes 90 et 92). De ce message sont extraits la valeur N du compteur CAC et le numéro d'identification  
30 ID du porteur de la carte SIM.

L'évaluation du risque est effectuée par l'étape 96 en fonction de la valeur N, du porteur de la carte et d'autres paramètres spécifiques 102.

Si l'évaluation du risque est considérée comme  
35 élevée par l'étape 98, la décision est de bloquer

l'usage de la carte (étape 100) en envoyant à la carte un message 40 de blocage.

Si l'évaluation n'est pas considérée comme élevée, la décision est d'autoriser l'usage de la carte (étape 102) en envoyant à la carte un message 40 d'autorisation. Ce message d'autorisation peut contenir d'autres éléments pour, par exemple, remettre à zéro le compteur CAC ou y introduire un nombre déterminé par le module 34 du réseau.

La description qui vient d'être faite de l'invention montre que la mise en place de deux modules de gestion du risque, l'un 32 dans la carte SIM et l'autre 34 dans le réseau, permet une souplesse de la gestion du risque, une partie par la carte à l'aide de paramètres simples à mettre en oeuvre (valeurs d'un compteur incrémenté et de seuils T0 et T1) et l'autre partie par le réseau en utilisant des paramètres plus sophistiqués qui peuvent être modifiés facilement.

La description ci-dessus montre qu'il est possible de définir un procédé qui comprend les étapes suivantes dans la carte à puce électronique 22 consistant à :

(a) vérifier (74) l'état bloqué ou non de la carte à puce électronique pour refuser (75) ou non la demande d'authentification ;

(b) dans le cas d'une autorisation de la demande d'authentification, compter (76) le nombre N de demandes d'authentification de la carte à puce électronique (22, SIM) par le réseau (54),

(c) comparer le nombre N de demandes d'authentification à un premier seuil T0,

(d) calculer un certificat cryptographique si  $N < T0$  et le transmettre au réseau,

(e) comparer le nombre N à un deuxième seuil T1 si  $N \geq T0$ ,

(f) mettre la carte à puce électronique (22, SIM) à l'état bloqué (82, 58) si  $N \geq T1$ , et

(g) calculer un certificat cryptographique (88) et élaborer un message de demande d'évaluation du risque (86) et les transmettre (38, 56) au réseau si  $T0 < N \leq T1$ .

Les étapes ci-dessus sont complétées dans le réseau par les étapes suivantes consistant à :

(h) analyser (94) le message de demande d'évaluation du risque transmis par la carte à puce électronique (22),

(i) évaluer (96, 102, 98) le risque en fonction des résultats de l'analyse selon l'étape précédente (h) et de paramètres spécifiques, et

(j) élaborer (100, 104, 40) un message de réponse et le transmettre à la carte à puce électronique (22).

L'invention a été décrite en supposant que le certificat cryptographique est calculé à partir d'un nombre aléatoire NA mais il est clair que ce nombre aléatoire peut être remplacé par un nombre qui ne serait pas aléatoire.

Par ailleurs, l'exemple particulier qui a été décrit est relatif à la détection d'accès de caractère frauduleux par leur nombre élevé ; cependant, l'invention s'applique aussi à la détection d'autres conditions qui correspondraient à d'autres types d'accès qui constitueraient un risque pour l'opérateur du réseau tels que le dépassement d'un crédit alloué à l'utilisateur d'une carte à prépaiement. Dans ce cas, les seuils  $T0$  et  $T1$  seraient des valeurs monétaires tandis que le compteur serait un accumulateur des dépenses effectuées par l'utilisateur du combiné. Ainsi,  $T0$  serait un seuil de dépenses autorisées tandis que  $T1$  serait un seuil au-delà duquel les dépenses ne seraient plus autorisées.

## R E V E N D I C A T I O N S

1. Système de gestion du risque dans un réseau de téléphonie mobile équipé d'un dispositif de service de messages (18), les combinés mobiles (14) comportant chacun une carte à puce électronique (22) (SIM) capable  
5 de calculer un certificat cryptographique d'authentification à partir d'une valeur fournie par le réseau, caractérisé :

- en ce que la carte à puce électronique (22, SIM) comprend des moyens (32) pour autoriser ou non le  
10 calcul d'un certificat cryptographique et sa transmission (56) au réseau lorsque certaines conditions sont remplies ou non et pour transmettre au réseau un message (38) de demande d'évaluation du risque lorsque d'autres conditions sont remplies, et
- 15 - en ce que le réseau (54) comprend des moyens (34) pour évaluer ledit risque en fonction des informations contenues dans le message (38) de demande d'évaluation du risque et de paramètres spécifiques à l'utilisateur du combiné mobile (14, ME) et pour envoyer un message  
20 (40) auxdits moyens (32) de la carte à puce électronique pour autoriser ou non le calcul et la transmission du certificat cryptographique.

2. Procédé pour mettre en oeuvre le système de gestion du risque selon la revendication 1, caractérisé  
25 en ce qu'il comprend, dans la carte à puce électronique (22), les étapes suivantes consistant à :

(a) vérifier (74) l'état bloqué ou non de la carte à puce électronique pour refuser (75) ou non la demande  
30 d'authentification,

(b) dans le cas d'une autorisation de la demande d'authentification, compter (76) le nombre (N) de

demandes d'authentification de la carte à puce électronique (22, SIM) par le réseau (54),

(c) comparer le nombre (N) de demandes d'authentification à un premier seuil  $T_0$ ,

5 (d) calculer un certificat cryptographique si  $N < T_0$  et le transmettre au réseau,

(e) comparer le nombre N à un deuxième seuil  $T_1$  si  $N \geq T_0$ ,

10 (f) mettre la carte à puce électronique (22, SIM) à l'état bloqué (82, 58) si  $N \geq T_1$ , et

(g) calculer un certificat cryptographique (88) et élaborer un message de demande d'évaluation du risque (86) et les transmettre (38, 56) au réseau si  $T_0 < N \leq T_1$ .

15

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend, en outre, les étapes suivantes mises en oeuvre par le réseau (54) consistant à :

20 (h) analyser (94) le message de demande d'évaluation du risque transmis par la carte à puce électronique (22),

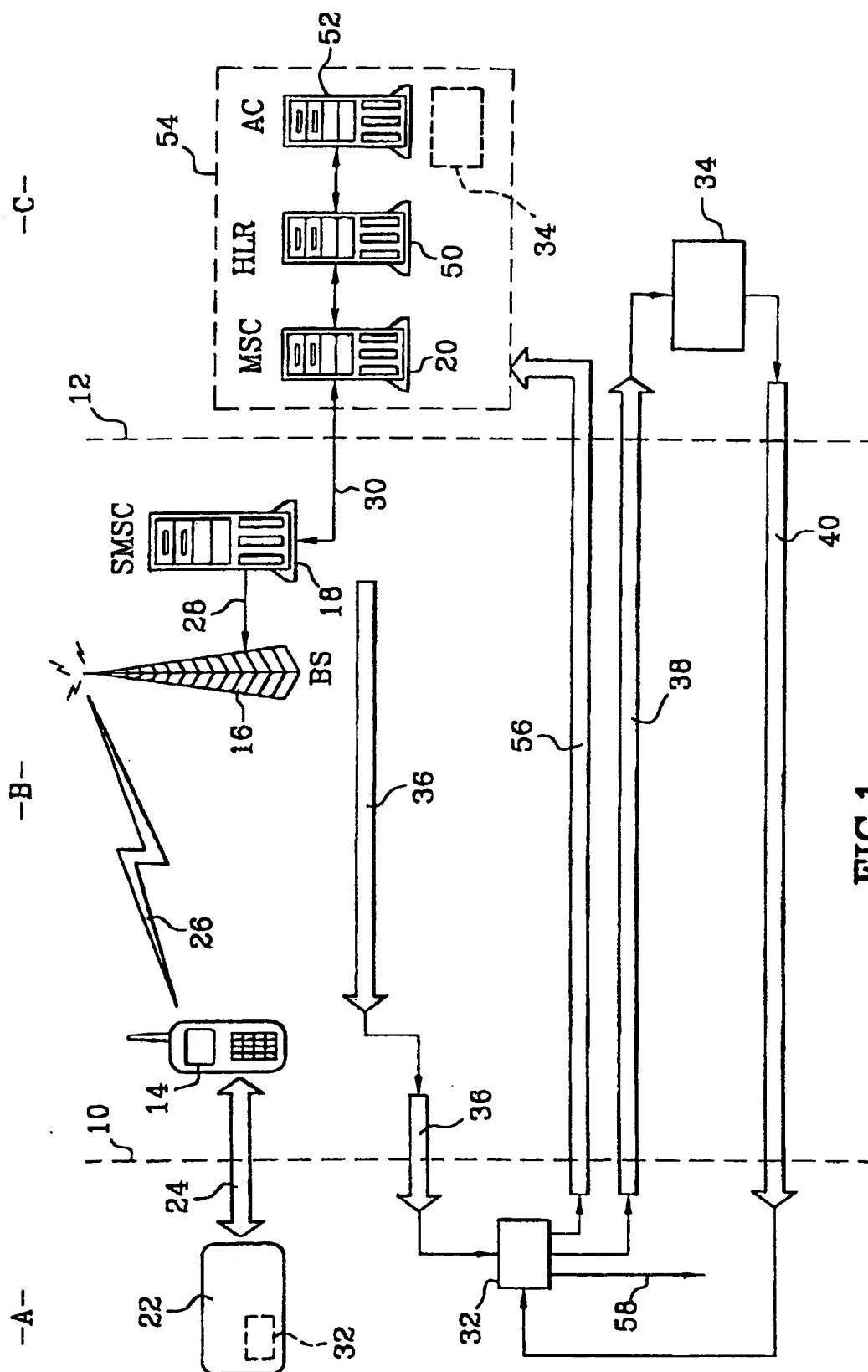
(i) évaluer (96, 102, 98) le risque en fonction des résultats de l'analyse selon l'étape précédente (h) et de paramètres spécifiques à l'utilisateur du combiné mobile, et

25

(j) élaborer (100, 104, 40) un message de réponse et le transmettre à la carte à puce électronique (22).

30 4. Procédé selon l'une des revendications précédentes 2 ou 3, caractérisé en ce que les nombres N,  $T_0$  et  $T_1$  sont des valeurs monétaires correspondant respectivement à une accumulation des dépenses effectuées en communications téléphoniques, un premier seuil de dépenses autorisées et un deuxième seuil au-

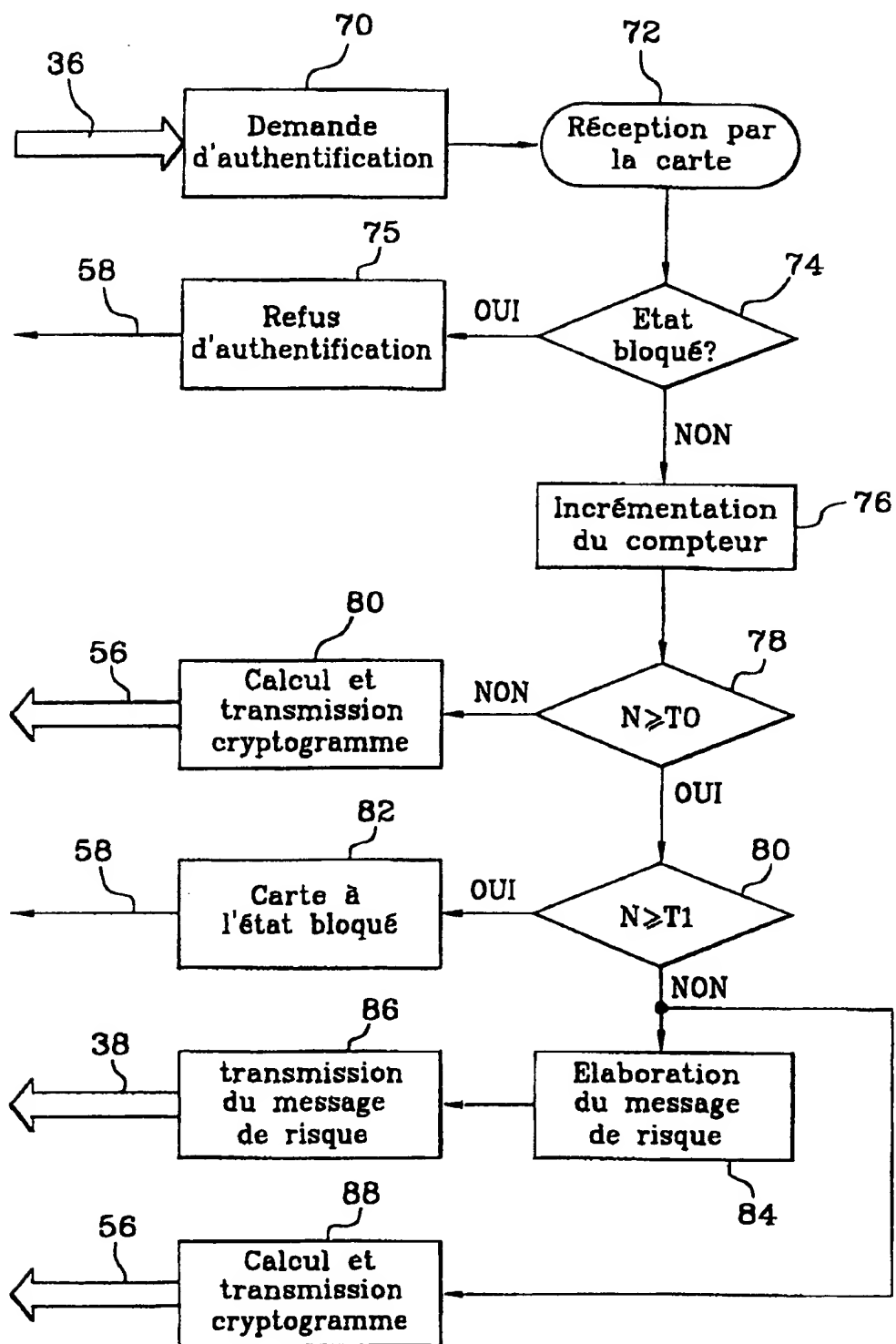
35 delà duquel les dépenses ne sont plus autorisées.



**FIG. 1**

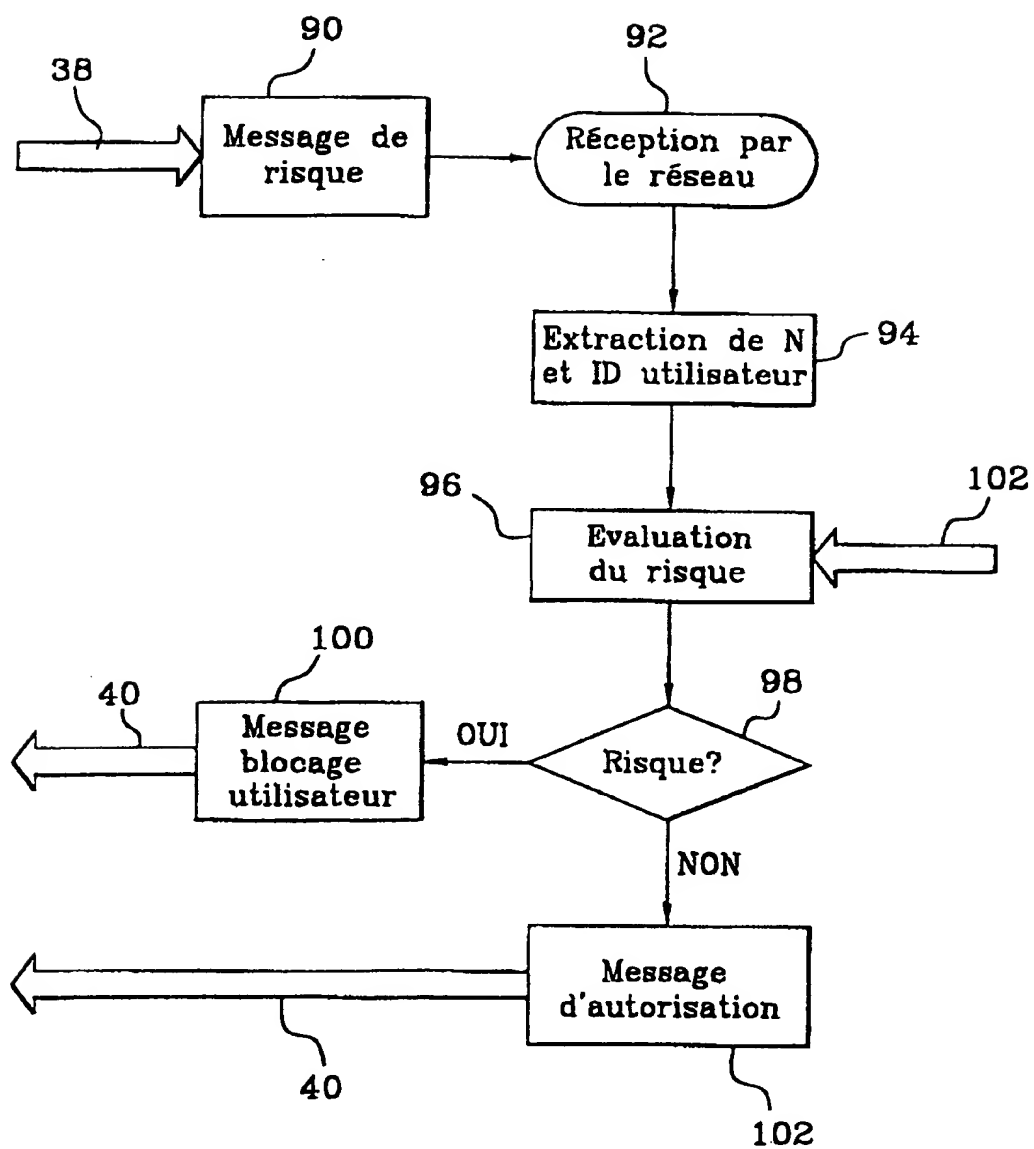
**THIS PAGE BLANK (USPTO)**

2/3

**FIG.2**

**THIS PAGE BLANK (USPTO)**

3/3

**FIG.3**

**THIS PAGE BLANK (USPTO)**